UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,262	01/11/2002	Jun Kamada	826.1783	6257

21171 7590 09/10/2007
STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
AUGUSTIN, EVENS J	
ART UNIT	**PAPER NUMBER**
3621	
MAIL DATE	**DELIVERY MODE**
09/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/042,262	**Applicant(s)** KAMADA ET AL.	
	Examiner Evens Augustin	**Art Unit** 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Acknowledgements

1. This is in response to an amendment filed on 14 June 2007. Claim 22 has been added. Claims 1-22 are pending. The 112 rejection has been withdrawn.

Response to Arguments

2. The United States Patent and Trademark Office has fully considered the applicant's arguments filed on 14 June 2007, but has not found those arguments to be persuasive.

   A. The prior art by Ginter teaches an environment that can recognize (differentiate or discriminate), process and store secure and non-secure data (col. 80, lines 20-67). It also manages allocation, deallocation, sharing and/or use of memory (col. 88, lines 63-65)- During the reply filed on 08 January 2007, applicant admitted that task allocation necessarily has the aspect discriminating (inherent). Applicant states - *the specification clearly states that the secure task management and the secure memory management allocate secure tasks and unsecured tasks. Therefore, the encrypted codes of the secure tasks are stored in the secure memory, and the codes of the unsecured tasks are stored in the normal memory.* <u>*As allocation necessarily involves discriminating*</u> *(otherwise, a determination cannot be made as to what tasks should be allocated to what memory), Applicants respectfully submit that the claim term discriminating is fully supported by the specification.* Therefore, "allocating" and "discriminating" will be used interchangeably- **("discriminating between the secure task and the normal task")**

B. Memories stores encrypted and unprotected content (column 21, lines 22-37) **("storing the encrypted code of the secure task")**

C. Verifying information by enforcing hardware compartmentalization/allocation of the secure execution space (e.g., preventing/not allowing a less trusted task from modifying a more trusted task) (col. 69, lines 10-15) **("verifying information for verification of validity of the encrypted code in a secure memory")**; **("allowing the secure processor to execute the encrypted code when the validity of the encrypted code is verified according to the verifying information")**Application stands finally rejected.

Claim Interpretation

3. In determining patentability of an invention over the prior art, the USPTO has considered all claimed limitations, and interpreted as broadly as their terms reasonably allow. Additionally, all words in the claims have been considered in judging the patentability of the claims against the prior art.

4. It should also be noted that, in the office action that:

   A. Items in the rejection that are in quotation marks are claimed language/limitations

   B. Passages in prior art references may be mere rephrasing/rewording of claimed limitations, but the implicit/explicit meaning of the references vis-à-vis the claimed limitation remains intact.

C. Functional recitation(s) using the word "for" or other functional terms have been considered but given less patentable weight[1] because they fail to add any steps and are thereby regarded as intended use language. To be especially clear, the Examiner has considered all claim limitations. However the A recitation of the intended use of the claimed invention must result in additional steps. See *Bristol-Myers Squibb Co. v. Ben Venue Laboratories, Inc.*, 246 F.3d 1368, 1375-76, 58 USPQ2d 1508, 1513 (Fed. Cir. 2001) (Where the language in a method claim states only a purpose and intended result, the expression does not result in a manipulative difference in the steps of the claim.).

D. Word(s) that are separated by "/" are being examined as being synonymous or equivalent

E. The United States Patent and Trademark Office (USPTO) is analyzing the claimed invention as a content/software/program/code distribution system between a content/software/program/code owner, a distributor or store and end users. The distributor pays a fee for the content/software/program/code that gets distributed to an end user with a multiprocessor machine. The invention describes the architecture of the multiprocessor system vis a vis the content/software/program/code. The invention describes the aspects of the encryption and verification (respectively) of the content/software/program/code within the user multiprocessor system.

[1] See *e.g. In re Gulack*, 703 F.2d 1381, 217 USPQ 401, 404 (Fed. Cir. 1983)(stating that although all limitations must be considered, not all limitations are entitled to patentable weight).

F. The USPTO interprets claim limitations that contain statement(s) such as "*if, may, might, can, could, when, potentially, possibly*", as optional language (this list of examples is not intended to be exhaustive). As matter of linguistic precision, optional claim elements do not narrow claim limitations, since they can always be omitted *(In re Johnston*, 77 USPQ2d 1788 (Fed. Circ. 2006)). They will be given less patentable weight, because language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation.

G. Independent claims are examined together, since they are not patentable distinct. If applicant expressly states on the record that two or more independent and distinct inventions are claimed in a single application, the Examiner may require the applicant to elect an invention to which the claims will be restricted.

H. Any official notices taken by the USPTO that are not adequately traversed by applicant will be taken to be admitted prior art.

I. The USPTO interprets common computer related words that are not lexicographically defined in accordance to Computer Dictionary, 3rd Edition, Microsoft Press, Redmond, WA, 1997[2]. The USPTO also uses published patent applications and

[2] Based upon Applicants' disclosure, the art of record, and the knowledge of one of ordinary skill in this art as determined by the factors discussed in MPEP §2141.03 (where practical), the Examiner finds that the *Microsoft Press Computer Dictionary* is an appropriate technical dictionary known to be used by one of ordinary skill in this art. See *e.g. Altiris Inc. v. Symantec Corp.*, 318 F.3d 1363, 1373, 65 USPQ2d 1865, 1872 (Fed. Cir. 2003) where the Federal Circuit used the *Microsoft Press Computer Dictionary* (3d ed.) as "a technical dictionary" to define the term "flag." See also *In re Barr*, 444 F.2d 588, 170 USPQ 330 (CCPA 1971)(noting that its appropriate to use technical dictionaries in order to ascertain the meaning of a term of art) and MPEP §2173.05(a) titled 'New Terminology.'

issued patents as well, for meanings of common computer related words that are not lexicographically defined. The aspect of "Task allocation" is being interpreted synonymously with memory management/allocation. ***Memory Management:*** n. 1. In operating systems for personal computers, procedures for optimizing the use of RAM (random access memory). **These procedures include selectively storing data,** monitoring it carefully, and freeing memory when the data is no longer needed.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requires of this title.

6. Claim 22 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

7. As per claim22, the preambles recite, "executing encrypted codes", however, do not recite that the computer program is encoded or recorded on a physical medium readable by a computer. Thus, the claims are directed to functionally descriptive material that is not functionally or structurally interrelated to the medium. Data structures not claimed as embodied in computer readable media (defined as "a collective word for the physical material, such as paper, disk, and tape, used for storing computer-based information", Microsoft Press, Computer Dictionary, Second Edition, © 1994) are descriptive material per se and are not statutory because they are neither physical "things" nor statutory processes.

Such claimed data structures do no define any structural and functional interrelationships between the data structure. See MPEP 2106(IV)(B)(1)(a).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States. . . .
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States. . . .
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

> subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter et al. (U.S 6427140).

2. As per claims 1-22, Ginter et al. discloses a invention that relates to computer-based and other electronic appliance-based technologies that help to ensure that information is accessed and/or otherwise used only in authorized ways, and maintains the integrity, availability, and/or confidentiality of such information and processes related to such use computer system that relates to development architecture frameworks, and more particularly to managing an environment of a development framework. The invention comprises of the following:

D. An environment for electronic information owners, distributors, and users; financial clearinghouses; and usage information analyzers and resellers (column 3, lines 45-48)

E. Multiprocessing system with multiprocessors (column 73, lines 38-40), in which content/software/program/code is encrypted through the components of the multiprocessor system (column 72, lines 31-67, column 73, lines 24-33)

F. Ginter et al. teaches Memory Management Unit that provides hardware support for memory management and virtual memory management functions. It may also provide heightened security by enforcing hardware compartmentalization/allocation of the secure execution space (e.g., to prevent a less trusted task from modifying a more trusted task) (col. 69, lines 10-15). Basically, Ginter et al. compartmentalizes/separates the execution of secured/trusted/encrypted from the less trusted/unsecured/unencrypted/normal tasks. Additionally, Ginter et al. teach the aspect of allocating task or task manager (column 83, line 36, column 88, lines 51-

67). The prior art by Ginter et al. has self-contained computing and processing environments that may include their own operating system kernel including code and data processing resources (column 79, lines 34-37). A kernel manages the basic hardware resources of electronic appliance, and controls the basic tasking provided by the operating system (col. 88, lines 51-53). It also manages allocation, deallocation, sharing and/or use of memory (col. 88, lines 63-65). The environment can recognize (differentiate or discriminate), process and store secure and non-secure data (col. 80, lines 20-67) **("a secure memory storing an encrypted code of a secure task and verifying information for verification of validity of the encrypted code") ("a secure processor executing the encrypted code when the validity of the encrypted code is verified according to the verifying information") ("a normal memory storing a code of a normal task; a normal processor executing the code of the normal task")**

G. The Examiner takes official notice that the aspect of using a normal memory for normal tasks and a secure memory for secure tasks (memory allocation) is common knowledge in the art (See US 5734822, col. 15, lines 15-25 -- US 6081876 col. 2, lines 8-15 –US 651162, col. 10, lines 53-67, col. 11, lines 1-8) **("a secure processor executing the encrypted code when the validity of the encrypted code is verified according to the verifying information") ("a normal memory storing a code of a normal task; a normal processor executing the code of the normal task")**

H. The environment can recognize (differentiate or discriminate), process and store secure and non-secure data (col. 80, lines 20-67). It also manages allocation, deallocation, sharing and/or use of memory (col. 88, lines 63-65)- During the reply filed on 08 January 2007, applicant admitted that task allocation necessarily has the aspect discriminating (inherent). Applicant states - *the specification clearly states that the secure task management and the secure memory management allocate secure tasks and unsecured tasks. Therefore, the encrypted codes of the secure tasks are stored in the secure memory, and the codes of the unsecured tasks are stored in the normal memory.* <u>*As allocation necessarily involves discriminating*</u> *(otherwise, a determination cannot be made as to what tasks should be allocated to what memory), Applicants respectfully submit that the claim term discriminating is fully supported by the specification.* Therefore, "allocating" and "discriminating" will be used interchangeably- **("discriminating between the secure task and the normal task")**

I. Memories stores encrypted and unprotected content (column 21, lines 22-37) **("storing the encrypted code of the secure task")**

J. Verifying information by enforcing hardware compartmentalization/allocation of the secure execution space (e.g., preventing/not allowing a less trusted task from modifying a more trusted task) (col. 69, lines 10-15) **("verifying information for verification of validity of the encrypted code in a secure memory"); ("allowing the secure processor to execute the encrypted code when the validity of the encrypted code is verified according to the verifying information")**

K. Content/software/program/code being stored in units of physical allocation memory (bytes) (column 68, line 51) and verified through the components of the multiprocessor system (column 125, lines 60-67) **("secure memory stores the**

encrypted code in units of physical memory allocation, stores the verifying information for the encrypted code in the units, and verifies the encrypted code in the units according to the verifying information, and the secure processor fetches, decrypts, and executes an encrypted instruction included in an encrypted code whose validity has been verified")

L. The system also uses digital signature to authenticate the communication of content (column 22, lines 5-10)

M. Employing a plurality of encryption keys (column 21, lines 65-67, column 22, lines 1-10, column 49, lines 1-59), in an non-volatile memory (column 49, lines 9-12) **("a plurality of decryption keys, and decrypts the encrypted instruction using a specified decryption key in the plurality of decryption keys")**

N. The aspects of using session keys (column 220, lines 20-21) **("secure memory and said secure processor share a session key after mutual authentication")**

O. System uses secure hardware (including drives) with a secure/trusted architecture (column 13, lines 5-25) **("a secure drive further encrypting the encrypted code using a unique key, and storing the encrypted code, wherein said secure drive and said secure memory share a session key after mutual authentication, said secure drive decrypts the encrypted code using the unique key at a read instruction from said controller, encrypts the code using the session key, and transfers the code to said secure memory")**

P. The storing of secure and non-secure information can be stored in a single memory chip or overlapping each other (par. 63, lines 40-43) **("at least parts of said secure memory and said normal memory overlap each other")**

Q. The system uses a memory management unit to manage the execution space (column 69, lines 9-42) **("secure processor fixes at least a part of a logical circuit for executing an encrypted code in a circuit state in a non-volatile manner using the encrypted code.")**

R. System teaches Electrically Erasable Programmable Read Only (EEPROM) (column 70, lines 66-67, column 71, lines 1-5) **("said secure processor erases a previous circuit state of the logical circuit, and newly overwrites the state.")**

S. Circuitry designed to "zeroize" memory may be included as an aspect of self-destruct processes (column 64, lines 30-31)

Conclusion

10. **THIS ACTION IS MADE FINAL.** Any new ground(s) of rejection is due to the applicant's amendment. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

11. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will

expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Evens Augustin whose telephone number is 571-272-6860. The examiner can normally be reached on Monday thru Friday 8 to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571-272-6779.

/ Evens J. Augustin/
Evens J. Augustin
September 2, 2007
Art Unit 3621

AFischer 9/4/07

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600